KANTON
LUZERN

Kantonale Datenschutzbeauftragte
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 61 00
datenschutz@lu.ch
www.datenschutz.lu.ch

Luzern, 01.09.2025

Management Summary
Datenschutzrechtliche und institutionelle Einschätzung zu M365

Die kantonale Datenschutzaufsicht Luzern nimmt angesichts der verstärkten Einführung von M365 der Firma Microsoft in öffentlichen Verwaltungen Stellung zur datenschutzrechtlichen Zulässigkeit und den strategischen Implikationen dieser Cloud-Plattform. Bei M365 handelt es sich nicht um eine herkömmliche Bürosoftware, sondern um eine umfassende digitale Arbeitsumgebung inklusive Kollaboration und Telefonie, deren Betrieb und Datenbearbeitung vollständig durch den global tätigen Anbieter Microsoft erfolgt. Damit sind weitreichende technische, rechtliche und politische Abhängigkeiten verbunden, welche die datenschutzrechtliche Bewertung massgeblich beeinflussen.

Aus heutiger Sicht ist der Einsatz von M365 zur Bearbeitung besonders schützenswerter Personendaten nicht zulässig. Es fehlt an einer hinreichend bestimmten gesetzlichen Grundlage, wie sie für schwerwiegende Eingriffe in die informationelle Selbstbestimmung nach Art. 36 Abs. 1 BV zwingend erforderlich ist. Die geltenden Bestimmungen des kantonalen Datenschutzgesetzes (KDSG) und seiner Verordnung (KDSV) reichen nicht aus, um die Bearbeitung solcher Daten in einer transnational regulierten Cloud-Infrastruktur zu legitimieren. Darüber hinaus verliert die öffentliche Verwaltung mit dem Einsatz von M365 in relevanten Teilen die Kontrolle über die Datenbearbeitung, was mit den datenschutzrechtlichen Anforderungen an Weisungsgebundenheit, Transparenz und effektive Kontrollmöglichkeiten nicht vereinbar ist.

Besonders problematisch ist zudem die rechtliche Lage im Zusammenhang mit Daten, die einer gesetzlichen Geheimhaltungspflicht unterliegen, etwa im Rahmen des Berufsgeheimnisses oder des Amtsgeheimnisses gemäss Strafgesetzbuch. Microsoft kann mangels organisatorischer, funktionaler und persönlicher Eingliederung nicht als strafrechtlich privilegierte Hilfsperson anerkannt werden. Die Auslagerung solcher Datenbearbeitungen an M365 stellt damit ein strafrechtlich relevantes Offenbaren dar, welches weder durch Datenschutzverträge noch durch technische Schutzmassnahmen wie Verschlüsselung (bei welcher Microsoft Zugang zu den Schlüsseln hat) gerechtfertigt

werden kann, solange der Anbieter potenziellen Zugriff auf die Daten hat oder dieser nicht ausgeschlossen werden kann.

Neben den datenschutzrechtlichen Erwägungen steht auch die digitale Souveränität öffentlicher Institutionen zur Diskussion. Die umfassende Nutzung von M365 bedeutet eine einseitige Abhängigkeit von einem privatwirtschaftlichen Anbieter, bei dem weder eine vertragliche Steuerung auf Augenhöhe noch ein verlässlicher Rückzug möglich ist. Damit wird nicht nur die rechtliche, sondern auch die politische Steuerungsfähigkeit über zentrale digitale Infrastrukturen geschwächt. Die Strategie Digitale Verwaltung Schweiz 2024–2027 fordert ausdrücklich die Wahrung digitaler Souveränität. Dieses Ziel kann nicht erreicht werden, wenn zentrale Verwaltungsfunktionen vollständig auf externe, extraterritorial regulierte Anbieter ausgelagert werden.

Die kantonale Datenschutzaufsicht empfiehlt daher, den Einsatz von M365 differenziert zu prüfen. Besonders schützenswerte Personendaten sowie Daten unter Geheimhaltungspflicht sind prioritär in Fachanwendungen oder lokal betriebenen Systemen zu bearbeiten. Vor einer Einführung sind datenschutzrechtliche Risiken umfassend zu bewerten, alternative Lösungen aktiv zu prüfen und die digitale Selbstbestimmung als strategisches Ziel institutionell zu verankern. Die Datenschutzaufsicht unterstützt öffentliche Organe dabei, tragfähige und rechtskonforme Lösungen zu entwickeln, welche technologischen Fortschritt und Grundrechtsschutz miteinander in Einklang bringen.

Detaillierte Erläuterungen über die datenschutzrechtliche und institutionelle Einschätzung zu M365

Die kantonale Datenschutzbeauftragte wird derzeit vermehrt mit Fragen zur Einführung und Nutzung von Microsoft 365 Cloud-Services (M365) in der öffentlichen Verwaltung konfrontiert. Zahlreiche Verwaltungsstellen planen die Integration von M365 oder befinden sich bereits in der Umsetzungsphase. Vor diesem Hintergrund erscheint es angezeigt, die datenschutzrechtliche Einschätzung und Haltung der kantonalen Datenschutzaufsicht in Bezug auf den Einsatz von M365 transparent darzulegen.

Das vorliegende Papier dient dazu, die Position der Aufsichtsbehörde nachvollziehbar und systematisch zu erläutern. Es basiert auf den geltenden datenschutzrechtlichen Vorgaben im Kanton Luzern (Kantonales Datenschutzgesetz, KDSG und Kantonale Datenschutzverordnung, KDSV), bezieht aber auch bundesrechtliche und verfassungsrechtliche Grundlagen sowie übergeordnete Prinzipien wie das der Verhältnismässigkeit mit ein. Darüber hinaus werden Fragestellungen zur Bearbeitung von besonders schützenswerten Personendaten, der Geheimnisschutzpflicht, zur digitalen Souveränität und zu aktuellen technologischen Entwicklungen berücksichtigt.

Die Veröffentlichung dieses Haltungspapiers verfolgt das Ziel, Verwaltungen, Fachverantwortlichen und Entscheidungsträgern eine fundierte Orientierungshilfe zu bieten. Gleichzeitig soll es den fachlichen Dialog fördern und zur Entwicklung tragfähiger, rechtlich abgesicherter Lösungen im Umgang mit cloudbasierten Anwendungen wie M365 beitragen.

Für Eilige ist zu Beginn ein Management Summary verfügbar.

1 Was ist M365?

M365 (manchmal auch Microsoft 365) ist die Bezeichnung der umfangreichen Cloud-Services von Microsoft. Anstelle der lokal, im eigenen Rechenzentrum betriebenen Anwendungen (On-Premises Software) wird die Software als Service (Software-as-a-Service, SaaS) bei Microsoft bezogen. Es findet damit grundsätzlich keine Installation und IT-Betrieb durch die interne Informatikabteilung statt, sondern die Softwarelösungen sind im Rechenzentrum der Microsoft installiert und werden durch MS betrieben.[1]
Zu den M365 Cloud-Services von Microsoft gehören neben den klassischen MS Office Anwendungen wie Word, PowerPoint oder Excel auch viele weitere Lösungen, insbesondere im Bereich der Kollaboration (Zusammenarbeit) wie Teams für Telefonate und Videokonferenzen, Outlook und Exchange Online für E-Mails und Datenablagen in der Cloud wie OneDrive oder SharePoint Online. Bei M365 handelt sich also nicht um eine simple Software für die Textverarbeitung oder Tabellenkalkulation, sondern um eine Software-Suite für eine umfassende Büroautomation und Kollaboration. Microsoft bietet diese Software-Suite den Unternehmen und Organisationen als Clouddienst in verschiedenen Enterprise-Lizenzen an. Zudem ist in den Enterprise-Lizenzen auch das Betriebssystem Windows mitlizenziert.

[1] Sehr wohl kann und soll Office 365 (d.h. Word, Excel, Access, PowerPoint, etc.) aktuell lokal installiert und betrieben werden. Hier scheint jedoch ebenfalls absehbar, dass dies nicht längerfristig der Fall sein sollte.

Neu enthalten in den Enterprise-Lizenzen ist auch «Microsoft Copilot for Microsoft 365». Copilot ist eine durch Künstliche Intelligenz (KI) gestützte Assistenzfunktion, die in die Microsoft 365-Anwendungen integriert ist. Es nutzt fortschrittliche KI-Technologien, um Nutzern bei der Erstellung, Bearbeitung und Verwaltung von Inhalten in den verschiedenen M365-Programmen zu helfen.

2 M365 alles Cloud?

Bis vor etwa 10 Jahren war die Mehrheit der Software von Microsoft lokal installiert, und Kunden erwarben einmalig Lizenzen für Produkte wie Windows, Office und Server-Software wie Exchange oder SharePoint. Microsofts Geschäftsmodell basierte auf dem Verkauf dieser Einzellizenzen und periodischen Updates. Dies änderte sich grundlegend mit dem strategischen Schwenk zur Cloud und dem Software-as-a-Service (SaaS)-Modell. Die Anfänge der Cloud-Strategie von Microsoft begannen zwischen 2010 und 2013. Mit der Einführung von Office 365 im Jahr 2011 brachte Microsoft einen Abonnementservice auf den Markt, der cloudbasierte Versionen der traditionellen Office-Anwendungen bot. Dies markierte den Beginn der Transformation hin zu einem SaaS-Modell. Im Jahr 2014 verstärkte Microsoft seinen Fokus auf Cloud-Technologien und erhöhte seine Ausgaben für Forschung und Entwicklung im Cloud-Bereich erheblich, bis hin zur heute praktizierten "Mobile First, Cloud First"-Strategie. Insgesamt hat Microsoft in den letzten zehn Jahren seine Geschäftsstrategie radikal umgestellt, von einem Modell, das auf dem Verkauf von Einzellizenzen für lokal installierte Software basierte, hin zu einem cloudbasierten SaaS-Modell. Heute ist Microsoft einer der führenden Anbieter von Cloud-Diensten weltweit, mit einem umfassenden Angebot an cloudbasierten Produkten und Dienstleistungen.
Mit dem abonnementsbasierten M365 erwirbt ein Kunde neben den Cloud-Diensten auch lokal installierbare Software wie die klassischen Microsoft Office Produkte Word, Excel, PowerPoint und Outlook aber auch das Betriebssystem Windows. Lange Zeit war unklar, ob diese Killerapplikationen zukünftig weiterhin mit einer einmaligen Lizenz erworben werden können oder nur noch im Abonnement. Microsoft Office 2021 war die letzte Version mit einer dauerhaften Lizenz. Seit April 2025 ist nun bekannt, dass Microsoft eine Office 2024 Version anbietet, welche mit einer Einmallizenz erworben werden kann und für welches der Support für fünf Jahre gewährleistet ist.[2]

In Gesprächen mit Verwaltungsstellen und IT-Dienstleistern zeigt sich immer wieder, dass hinsichtlich der Verfügbarkeit von lokal installierbarer Microsoft-Software teilweise Unklarheit oder Fehlannahmen bestehen. Häufig wird davon ausgegangen, Microsoft biete seine zentralen Produkte nur noch in der cloudbasierten Variante von M365 an. Diese Annahme ist nicht korrekt.

Tatsächlich sind zentrale Microsoft-Anwendungen auch weiterhin in On-Premises-Form verfügbar – also als lokal installierbare Software, die innerhalb der eigenen Infrastruktur betrieben werden kann. Neben der angekündigten Version Office 2024 LTSC mit Einmallizenz, stehen auch Exchange Server, SharePoint Server sowie Skype for Business Server weiterhin in sogenannten Subscription Editions (SE) zur Verfügung. Diese Produkte ermöglichen einen vollständigen Betrieb innerhalb der eigenen Infrastruktur, ohne Daten in die Microsoft-Cloud auslagern zu müssen.

[2] Übersicht über Office LTSC 2024 - Office | Microsoft Learn abgerufen am 24.06.2025.

Gleichwohl ist zu beobachten, dass Microsoft selbst wenig offensiv über die Verfügbarkeit und Zukunft dieser On-Premises-Produkte informiert. Die Kommunikation konzentriert sich stark auf cloudbasierte Angebote, was zur Folge hat, dass bei Entscheidungsträgern oft der Eindruck entsteht, es gebe keine ernstzunehmende Alternative zu M365. Diese strategische Zurückhaltung von Microsoft trägt dazu bei, dass die digitale Souveränität öffentlicher Stellen faktisch untergraben wird, noch bevor eine bewusste Entscheidung über die Betriebsform getroffen wurde.

Vor diesem Hintergrund erscheint es besonders wichtig, dass öffentliche Organe sich beim Technologieentscheid nicht ausschliesslich auf Anbieterkommunikation verlassen, sondern aktiv nach lokal betriebenen Alternativen suchen, etwa im Rahmen einer Marktevaluation oder durch unabhängige Beratung.

3 Besonders schützenswerte Personendaten

Die datenschutzrechtliche Bewertung des Einsatzes von Cloud-Diensten wie M365 zur Bearbeitung besonders schützenswerter Personendaten[3] ist aus rechtlicher Sicht differenziert vorzunehmen. Im Zentrum der Betrachtung steht das Zusammenspiel zwischen kantonalem Datenschutzrecht, insbesondere dem Gesetz über den Datenschutz im Kanton Luzern (KDSG) und seiner Verordnung (KDSV), den Vorgaben der Bundesverfassung (BV) sowie den Grundsätzen des modernen Datenschutzrechts, namentlich dem Prinzip der Verhältnismässigkeit.

Zunächst ist festzuhalten, dass die Bearbeitung besonders schützenswerte Personendaten gemäss § 2 Abs. 2 KDSG einen besonders intensiven Eingriff in die informationelle Selbstbestimmung der betroffenen Person darstellt. Die damit verbundene Grundrechtsrelevanz ist erheblich, insbesondere bei Daten über die Gesundheit, über sozialhilferechtliche Verhältnisse oder über besonders intime Aspekte der Persönlichkeit. In Anbetracht der Schwere eines solchen Eingriffs verlangt Art. 36 Abs. 1 der Bundesverfassung, dass eine hinreichend bestimmte gesetzliche Grundlage auf Stufe formelles Gesetz vorhanden sein muss, wenn ein schwerer Eingriff in ein Grundrecht erfolgen soll. Diese Voraussetzung erfüllt das geltende kantonale Datenschutzrecht in Bezug auf die Bearbeitung besonders schützenswerte Personendaten in einer komplexen, transnationalen Cloud-Infrastruktur nicht. Es existiert weder eine ausdrückliche noch eine ausreichend bestimmte gesetzliche Norm, die den Einsatz von M365 in diesem Kontext legitimieren könnte.

Weiterhin stellt die Nutzung von M365 in der üblichen Cloud-Architektur eine faktische Auslagerung der Datenbearbeitung an einen privatwirtschaftlichen Dritten dar, der seinen Hauptsitz ausserhalb des Geltungsbereichs des schweizerischen Datenschutzrechts hat. Aus datenschutzrechtlicher Perspektive ist dabei insbesondere problematisch, dass die tatsächliche Kontrolle über die Bearbeitungsvorgänge durch die Verwaltung in wesentlichen Teilen aufgegeben wird. Die gesetzlichen Anforderungen an eine rechtskonforme Auftragsbearbeitung – namentlich die jederzeitige Weisungsgebundenheit und die effektive Kontrolle über die Datenverwendung gemäss § 6 ff. KDSV – können unter diesen Bedingungen kaum erfüllt werden. Die technische Komplexität von M365, die Nutzung globaler Subunternehmerketten sowie die eingeschränkten Möglichkeiten zur Einsicht in konkrete Bearbeitungsprozesse führen

[3] Vgl. dazu das Merkblatt: Besonders schützenswerte Personendaten.

zu einem strukturellen Kontrollverlust, der mit den Prinzipien des Luzerner Datenschutzrechts nicht vereinbar ist.

Besondere Bedeutung kommt in diesem Zusammenhang dem verfassungsrechtlich und datenschutzrechtlich verankerten Verhältnismässigkeitsprinzip zu. Dieses verlangt, dass jede Datenbearbeitung zur Erreichung eines legitimen Zwecks geeignet, erforderlich und zumutbar sein muss. Der Einsatz von M365 zur Bearbeitung besonders schützenswerte Personendaten ist weder erforderlich noch verhältnismässig im engeren Sinne, sofern gleichwertige Alternativen zur Verfügung stehen, die mit geringerer Eingriffsintensität verbunden sind. In der Schweiz existieren sowohl staatliche wie auch private Cloud-Dienstleistungen, die eine lokalisierte, datenschutzkonforme Bearbeitung ermöglichen und den Anforderungen an Kontrolle, Datenhoheit und Weisungsbindung deutlich besser genügen. Solche Alternativen sind demnach vorrangig zu berücksichtigen, sofern sie den gleichen Zweck erfüllen. Zudem wird vielfach als risikominimierende Massnahme das «Primat der Fachanwendungen» propagiert, welches vorsieht, dass sensible Daten eben gerade nicht mit M365 bearbeitet werden, sondern diese in den Fachanwendungen verbleiben und auch nur dort bearbeitet werden. Es stehen mit den Fachanwendungen und lokal installierten MS Office Anwendungen gleichwertige Alternativen für die Bearbeitung von besonders schützenswerte Personendaten zur Verfügung.

Ein zusätzliches rechtliches Problem ergibt sich aus der Tatsache, dass Microsoft als Anbieter von M365 dem US-amerikanischen Recht unterliegt. Gesetze wie der US Cloud Act oder der Foreign Intelligence Surveillance Act (FISA) eröffnen ausländischen Behörden unter bestimmten Umständen Zugriffsmöglichkeiten auf in der Cloud gespeicherte Daten. Diese Zugriffsmöglichkeiten sind mit dem schweizerischen Begriff des "angemessenen Datenschutzes" gemäss KDSG und KDSV nicht vereinbar.

Besonders kritisch ist zudem der Versuch, den Schutzstatus besonders schützenswerte Personendaten durch eine verwaltungsinterne Klassifizierung weiter zu differenzieren, indem lediglich jene Informationen als „geheim" gelten sollen, deren Bekanntgabe gegenüber Unberechtigten «existenzgefährdende» Auswirkungen haben könnte. Eine solche interne Normsetzung läuft dem Legalitätsprinzip zuwider, da sie den gesetzlich vorgesehenen Schutzstandard relativiert. Weder das KDSG noch das DSG lassen eine Abstufung von besonders schützenswerte Personendaten zu, die den Schutz der betroffenen Person von der Einschätzung einer existenziellen Bedrohung abhängig macht. Sämtliche besonders schützenswerten Personendaten unterliegen einem normativ definierten, erhöhten Schutzbedarf, der nicht durch eine verwaltungsinterne Risikobewertung abgeschwächt werden darf. Das Vorliegen einer Bearbeitung von besonders schützenswerten Personendaten ebenso wie jene von speziellen Geheimnisnormen ergibt sich aus dem Gesetz selbst und lässt sich nicht mit einer «Datenklassifizierung» übersteuern.

Aus einer systematischen und rechtlichen Perspektive ist deshalb festzuhalten, dass die Bearbeitung besonders schützenswerter Personendaten in M365 unter den geltenden rechtlichen Rahmenbedingungen unzulässig ist, bzw. weiterführenden Schutzmassnahmen getroffen werden müssen, damit eine Bearbeitung mit M365 zulässig ist (z.B. Verschlüsselung mit Schlüsselzugriff ausschliesslich beim Organ). Dies gilt sowohl unter dem Gesichtspunkt der fehlenden gesetzlichen Grundlage als auch wegen mangelnder Kontrollierbarkeit, unverhältnismässiger Risiken und unzulässiger Drittstaatenübermittlung. Ein daten-

schutzkonformer Einsatz von Cloud-Lösungen bedarf in solchen Fällen einer spezifischen gesetzlichen Regelung sowie technischer und organisatorischer Massnahmen, welche die Einhaltung der datenschutzrechtlichen Grundprinzipien in vollem Umfang sicherstellen.

4 Personendaten unter einer Geheimnisnorm inkl. dem Berufsgeheimnis

Die Rechtsordnung sieht bei bestimmten Kategorien von Personendaten – etwa im Rahmen des Berufsgeheimnisses gemäss Art. 321 StGB oder des Amtsgeheimnisses gemäss Art. 320 StGB – einen erhöhten Schutzstandard vor. Während das Datenschutzrecht unter gewissen Voraussetzungen die Auslagerung der Datenbearbeitung an Dritte gestattet (insbesondere durch Auftragsdatenbearbeitung), ist dieser datenschutzrechtliche Spielraum durch die Schranken der Geheimnisschutznormen begrenzt. Der Geheimnisschutz entfaltet insoweit Tatbestands- und Rechtfertigungswirkung, die eigenständig und nicht durch datenschutzrechtliche Konstruktionen wie Weisungsbindung oder vertragliche Verschwiegenheitsverpflichtungen aufgehoben werden können.

Wie Prof. Dr. iur. Wolfgang Wohlers in seinem Gutachten über die Auslagerung einer Datenbearbeitung und Berufsgeheimnis[4] überzeugend darlegt, liegt beim Outsourcing der Datenbearbeitung an Dritte grundsätzlich ein „Offenbaren" im Sinne der Art. 320 und 321 StGB vor, sofern der Dritte nicht als Hilfsperson im strafrechtlichen Sinn gilt (siehe dazu auch das separate Kapitel weiter unten). Bei Cloud-Anbietern wie Microsoft, welche ausserhalb des funktionellen und organisatorischen Einflussbereichs des Geheimnisträgers stehen, fehlt es regelmässig an den Voraussetzungen für die Annahme einer strafrechtlich privilegierten Hilfsperson. Somit wird durch die Auslagerung an M365 – selbst bei Vorliegen von Vertragsklauseln zur Geheimhaltung – ein strafrechtlich geschütztes Geheimnis offenbart. Eine solche Offenbarung ist ohne ausdrückliche Einwilligung der betroffenen Person oder einer spezialgesetzlichen Grundlage nicht straflos.

Die Rechtfertigung durch ein überwiegendes berechtigtes Interesse – wie sie etwa bei internen technischen Notwendigkeiten in Betracht gezogen werden könnte – ist bei der Nutzung globaler Cloud-Infrastrukturen besonders problematisch. Eine solche Offenbarung ist in der Regel nicht zwingend erforderlich, da es technisch und organisatorisch mögliche Alternativen mit geringerem Risiko für die Integrität des Geheimnisschutzes gibt (z.B. inländische IT-Dienstleister mit vollständiger Weisungs- und Kontrollbindung). Bereits aus dem Verhältnismässigkeitsprinzip ergibt sich daher, dass die Offenbarung in der Cloud nicht zulässig ist, da mildere Mittel verfügbar wären. Es gelten sinngemäss dieselben Feststellungen zum Verhältnismässigkeitsprinzip bei der Bearbeitung von besonders schützenswerten Personendaten (siehe dazu das Kapitel über die besonders schützenswerten Personendaten).

Dr. Blonski hebt in ihrem Aufsatz «Cloud - alles Risiko»[5] hervor, dass insbesondere im Fall der Nutzung von Cloud-Diensten mit Serverstandorten ausserhalb der Schweiz – etwa in den USA – ein erheblicher Kontrollverlust über den Zugriff auf die Daten besteht. Die Anwendung von extraterritorialen Gesetzen wie dem US CLOUD Act erlaubt US-Behörden den Zugriff auf Daten, ohne dass dies über einen formalisierten Rechtshilfeweg erfolgt. Dieser Zugriff wider-

[4] Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Zürich/Basel/Genf 2016.
[5] Erschienen in der Schweizerische Juristen-Zeitung Nr. 20 | 15.10.2023.

spricht dem ordre public der Schweiz und dem Grundsatz der Rechtmässigkeit der Datenbearbeitung. Eine Auslagerung in solche Infrastrukturen ist daher nicht mit der Geheimhaltungspflicht vereinbar.

Ein zentraler Grundsatz des Geheimnisschutzes besteht darin, dass allein der Geheimnisherr – also die betroffene Person – bestimmen darf, mit wem das Geheimnis geteilt wird. Es ist nicht Sache des Geheimnisträgers, diesen Kreis einseitig zu erweitern. Das Einsetzen technischer oder organisatorischer Schutzmassnahmen – wie etwa Verschlüsselung – kann zwar das Risiko mindern, aber nicht die Offenbarungshandlung an sich verhindern, sofern der Cloud-Anbieter potentiell Zugriff erhalten kann oder Schlüsselmaterial nicht vollständig unter der Kontrolle des Geheimnisherrn bzw. des Geheimnisträgers bleibt.

4.1 Warum Microsoft keine strafrechtliche Hilfsperson nach Art. 321 StGB ist

Die strafrechtliche Hilfsperson im Rahmen von Art. 321 StGB ist eine ausnahmsweise privilegierte Drittperson, der enge organisatorische, funktionale und persönliche Bindungen zum Berufsgeheimnisträger zugeordnet werden können. Die Lehre und Rechtsprechung verlangen hierfür eine eingegliederte Vertrauensstellung, wie sie etwa bei einer medizinischen Assistentin, einem Anwaltssekretär oder einem internen IT-Techniker vorliegt. Microsoft als internationaler Konzern ist weder in die Organisation des Berufsgeheimnisträgers integriert, noch untersteht er dessen unmittelbarer Kontrolle oder Weisung, was Voraussetzung für eine strafrechtlich relevante Hilfspersonenqualität ist.

Die Hilfsperson muss gleichsam als verlängerte Hand des Geheimnisträgers tätig sein. Sie darf keinen eigenen Entscheidungsspielraum in der Datenbearbeitung haben und muss vollständig dem Weisungsrecht des Geheimnisträgers unterliegen. Bei Microsoft handelt es sich jedoch um einen eigenständig operierenden Cloud-Anbieter, der selbst Subunternehmer beiziehen kann und dessen Datenflüsse, Bearbeitungspfade und Sicherheitsvorkehrungen für den Auftraggeber nicht vollständig einsehbar oder kontrollierbar sind.

Selbst wenn technische Massnahmen wie Verschlüsselung verwendet werden, verbleibt ein Restrisiko des Zugriffs, insbesondere durch ausländische Behörden (Stichwort: US CLOUD Act). Der Geheimnisträger kann somit nicht ausschliessen, dass Dritte auf die geheimnisschutzpflichtigen Daten zugreifen – was bereits ausreicht, um die Schutzwirkung des Art. 321 StGB zu unterlaufen. Damit fehlt eine Grundvoraussetzung für die Privilegierung als Hilfsperson: die verlässliche Wahrung des Geheimnisses durch die beauftragte Stelle.

Wird Microsoft fälschlich als Hilfsperson eingestuft und es kommt dennoch zu einer Offenbarung oder unautorisierten Zugriffsmöglichkeit, liegt objektiv eine Verletzung von einschlägigen Geheimnisnormen (z.B. Berufs- bzw. Amtsgeheimnis) Berufsgeheimnisses vor. Dies kann zur strafrechtlichen Verantwortlichkeit des Geheimnisträgers führen, da der Schutzbereich von Art. 321 StGB bzw. Art. 320 StGB durch vertragliche Vereinbarungen oder private Interpretation nicht abgeändert werden kann.

Die Einstufung von Microsoft als Hilfsperson im Sinne von Art. 321 StGB ist rechtsdogmatisch unhaltbar. Sie würde den Schutzzweck der Strafnorm unterlaufen, wonach nur eng verbundene, tatsächlich kontrollierbare Personen mit dem Geheimnis betraut werden dürfen. Ein international agierender Cloud-Anbieter mit eigenem Datenzugriff und potenzieller Drittstaatenbindung erfüllt diese Voraussetzungen offenkundig nicht.

4.2 Schlussfolgerung

Die Bearbeitung von Personendaten, welche einer gesetzlichen Geheimhaltungspflicht unterliegen, ist in einer Cloud-Infrastruktur wie M365 aus mehreren Gründen nicht zulässig:

- Es handelt sich um ein strafrechtlich relevantes „Offenbaren", welches nicht durch Datenschutzverträge vereinbart bzw. wegbedungen werden kann.
- Es fehlt an einer tauglichen Rechtfertigung (nur im DSG, im KDSG nicht vorhanden) durch Einwilligung, spezialgesetzliche Grundlage oder überwiegendes Interesse.
- Die extraterritoriale Zugriffsmöglichkeit unterminiert die gesetzlich geforderte Vertraulichkeit.
- Die Entscheidung über die Weitergabe eines Geheimnisses kann nicht durch den Geheimnisträger delegiert werden, sondern verbleibt beim Geheimnisherrn.

5 Überlegungen zur Digitale Souveränität

Auch wenn die digitale Souveränität nicht primär zum Zuständigkeitsbereich der Datenschutzaufsicht gehört, erscheint es aus verwaltungsstrategischer und verfassungsrechtlicher Perspektive unerlässlich, das Thema in die datenschutzrechtliche Beurteilung der Nutzung von M365 einzubeziehen. Die Fähigkeit staatlicher Institutionen, digitale Systeme und Infrastrukturen eigenständig, kontrolliert und nachhaltig zu betreiben, berührt grundlegende Aspekte der staatlichen Selbstbestimmung und damit letztlich auch die Fähigkeit, datenschutzrechtliche Vorgaben effektiv umzusetzen.

Die Strategie Digitale Verwaltung Schweiz 2024–2027 misst der digitalen Souveränität einen zentralen Stellenwert bei. In diesem Kontext geht es nicht nur um technische Fragen der Systemarchitektur, sondern auch um rechtliche, organisatorische und politische Steuerungsfähigkeit über den gesamten Lebenszyklus digitaler Systeme und Datenbearbeitungen. Die Abhängigkeit von global agierenden Technologiekonzernen wie Microsoft, bei denen weder eine Vertragsgestaltung auf Augenhöhe noch ein sicherer Rückzugsmechanismus besteht, stellt die Grundidee digital souveränen Verwaltungshandelns infrage.

Vor diesem Hintergrund ist es sachlich und normativ gerechtfertigt, Überlegungen zur digitalen Souveränität in die Beurteilung der datenschutzrechtlichen Zulässigkeit von Cloud-Diensten einzubeziehen – nicht als selbstständiger Prüfpunkt, sondern als entscheidungsrelevanter Kontext, der das Mass an tatsächlicher Kontrolle und Verantwortung über Datenbearbeitung in wesentlicher Weise mitbestimmt.

Die Strategie Digitale Verwaltung Schweiz 2024 bis 2027[6] definiert die Digitale Souveränität wie folgt: «Fähigkeit von Bund, Kantonen, Städten und Gemeinden, digitale Behördenleistungen autonom nutzen und kontrollieren zu können. Dabei geht es um die Selbstbestimmung über den gesamten Lebenszyklus eines digitalen Systems, von der Konzeption über die Nutzung bis zur Stilllegung digitaler Systeme und der Daten, die bearbeitet und gespeichert werden, sowie der daraus resultierenden Prozesse.» Unter den Prinzipien der digitalen Verwaltung soll die Verwaltung auf ihre digitale Souveränität achten, um eine ausreichende und nachhaltige Kontrolle des digitalen Raums zu gewährleisten. Die Strategie nimmt auch Bezug

[6] https://www.fedlex.admin.ch/eli/fga/2024/45/de, abgerufen am 16.05.2024.

auf Cloud-Lösungen welche das «Cloud-enabled-Government» ermöglichen soll. Im Fokus steht dabei aber die digitale Souveränität (neben anderen Themenfeldern).

Mit der angedachten breiten Nutzung von M365 auf dem Desktop von Verwaltungsangestellten begeben sich die öffentlichen Organe in eine Herstellerabhängigkeit von noch nie dagewesenem Ausmass. Die öffentlichen Organe sind gegenüber Microsoft weder vertraglich, kommerziell, noch technisch souverän. Die ausgeprägte vertragliche, kommerzielle und technische Fremdbestimmtheit führen dazu, dass die Selbstbestimmung über den gesamten Lebenszyklus nicht gegeben ist. Erschwerend kommt hinzu, dass ein Ausstieg aus M365 im Notfall unmöglich scheint, weil valable Varianten vielfach nicht geprüft wurden oder gar nicht vorgesehen sind.

Das Datenschutzrecht geht davon aus, dass eine notwendige Vertragsverhandlung bei einer Auslagerung einer Datenbearbeitung auf Augenhöhe stattfinden kann. Dies ist bei Microsoft bekanntermassen nicht gegeben. Vertragliche Anpassungen sind durch das öffentliche Organ nicht möglich. Auch andere Länder bekunden zunehmend Mühe, von Microsoft verbindliche Informationen und Angaben zu erhalten.

5.1 Digitale Souveränität im Spannungsfeld geopolitischer Abhängigkeiten

Ein zentrales Anliegen der digitalen Souveränität besteht darin, staatliche Organe in die Lage zu versetzen, ihre digitalen Infrastrukturen unabhängig und ohne externe politische Einflussnahme betreiben zu können. Die «Strategie Digitale Verwaltung Schweiz 2024–2027» hebt diesen Grundsatz als Leitlinie für die digitale Transformation der öffentlichen Verwaltung hervor und betont die Notwendigkeit einer autonomen Steuerungs- und Entscheidungskompetenz über den gesamten Lebenszyklus digitaler Systeme.

In diesem Kontext rückt zunehmend auch die politische Resilienz gegenüber extraterritorialen Eingriffen in den Fokus. Der jüngst publik gewordene Fall, in dem Microsoft infolge von US-amerikanischen Sanktionsmassnahmen den Zugriff des Chefanklägers des Internationalen Strafgerichtshofs (IStGH) auf ein dienstliches M365 E-Mail-Konto sperrte, verdeutlicht exemplarisch, wie geopolitische Interessenlagen die Verfügbarkeit und Integrität digitaler Dienste beeinträchtigen können. Zwar handelt es sich dabei um einen völkerrechtlich-politischen Ausnahmefall, doch illustriert er strukturell die inhärente Verwundbarkeit öffentlicher Institutionen gegenüber einseitigen, ausländisch motivierten Interventionsmöglichkeiten.

Auch die Datenschutzbeauftragte des Kantons Basel-Stadt hat in einer Stellungnahme vom April 2025 auf diese Problematik hingewiesen.[7] Sie betont, dass die vollständige Auslagerung digitaler Arbeitsumgebungen – insbesondere in Form umfassender cloudbasierter Office-Suiten wie M365 – faktisch eine Abhängigkeit schafft, welche die digitale Selbstbestimmung staatlicher Stellen substantiell beeinträchtigt. Diese Abhängigkeit zeigt sich nicht nur in technischer oder vertraglicher Hinsicht, sondern zunehmend auch in Form politisch-institutioneller Asymmetrien, in denen der Zugang zu wichtigen Infrastrukturen von externen Akteuren beeinflusst oder gar blockiert werden kann.

Vor diesem Hintergrund erscheint es geboten, digitale Souveränität nicht allein im technologischen oder datenschutzrechtlichen Rahmen zu denken, sondern sie auch als strategisches Schutzziel verfassungsrechtlicher Tragweite zu verstehen. Die Nutzung digitaler Systeme darf

[7] https://www.bs.ch/news/2025-medienmitteilung-der-datenschutzbeauftragten-des-kantons-basel-stadt-zu-m365, abgerufen am 22.05.2025

nicht dazu führen, dass staatliche Organe in Situationen struktureller Abhängigkeit geraten, in denen sie weder die Funktionsfähigkeit ihrer Verwaltung noch den Schutz der ihnen anvertrauten Daten aus eigener Kraft sicherstellen können.

6 Fazit

Die datenschutzrechtliche und institutionelle Bewertung des Einsatzes von M365 im öffentlichen Sektor ergibt aus Sicht der kantonalen Datenschutzaufsicht ein klares Bild: Die Bearbeitung besonders schützenswerter Personendaten sowie von Personendaten, die einer gesetzlichen Geheimhaltungspflicht unterliegen, ist unter den derzeit gegebenen technischen, rechtlichen und politischen Rahmenbedingungen in der M365-Cloud-Infrastruktur nicht mit dem kantonalen Datenschutzrecht vereinbar. Die rechtlichen Grundlagen – namentlich § 6 ff. KDSV in Verbindung mit § 2 Abs. 2 KDSG sowie Art. 36 Abs. 1 BV – erfordern ein Schutzniveau, das im Kontext einer global vernetzten, extraterritorial regulierten Cloud-Architektur nicht gewährleistet werden kann.

Gleichzeitig zeigen die strukturellen Abhängigkeiten in der Nutzung von M365 – etwa bei Lizenzmodellen, technischen Standards oder vertraglicher Steuerbarkeit – erhebliche Defizite im Hinblick auf die digitale Souveränität öffentlicher Institutionen. In einer digitalisierten Verwaltung kann der Verlust faktischer und rechtlicher Kontrolle über zentrale IT-Infrastruktur nicht nur als organisationsstrategisches Risiko, sondern auch als grundrechtlich relevanter Souveränitätsverzicht verstanden werden.

Die kantonale Datenschutzbeauftragte ist sich bewusst, dass technologische Entwicklungen und Innovationsbestrebungen auch in der Verwaltung ein dynamisches Umfeld schaffen. Sie verfolgt daher mit ihrer Haltung zu M365 ausdrücklich das Ziel, eine offene, rechtsstaatlich fundierte und zukunftsfähige Diskussion zu ermöglichen. Sollte es in Einzelfällen zu abweichenden Bewertungen kommen, sieht sie es im Interesse der Rechtssicherheit und der Verwaltungsprofessionalität als sachgerecht an, die Zulässigkeit entsprechender Datenbearbeitungen gegebenenfalls im Dialog mit den betroffenen Stellen zu klären – und, wo erforderlich, auch im Rahmen der ihr gemäss KDSG zustehenden Kompetenzen formell zu beurteilen. Im Sinne der partnerschaftlichen Zusammenarbeit steht die Datenschutzaufsicht dabei jederzeit als konstruktive Ansprechpartnerin zur Verfügung – mit dem Ziel, tragfähige und rechtskonforme Lösungen zu ermöglichen.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Kontaktformular:	https://datenschutz.lu.ch/kontakt
Telefon:	+41 41 228 61 00
E-Mail:	datenschutz@lu.ch **WARNUNG**: Der E-Mail-Verkehr ist unsicher. Vertrauliches gehört deshalb nicht in E-Mails!
Website:	https://datenschutz.lu.ch/